

NUMBER THEORY

AMIN WITNO

Preface

Written at Philadelphia University, Jordan for Math 313, these notes¹ were used first time in the Fall 2005 semester. They have since been revised² and shall be revised again as often as the author teaches the course. Outline notes are more like a revision. No student is expected to fully benefit from these notes unless they have regularly attended the lectures.

1 Divisibility

The natural numbers $1, 2, 3, \dots$ together with their negatives and zero make up the set of *integers*. Number Theory is the study of integers. Every number represented throughout these notes will be understood an integer unless otherwise stated.

Definition. The number d divides m , or m is *divisible* by d , if the operation $m \div d$ yields an integer. This relation may be written $d \mid m$, or $d \nmid m$ if it is not true. When $d \mid m$, the number d is also called a *divisor* of m , and m a *multiple* of d . For example $3 \mid 18$ and $5 \nmid 18$. We may also state that even numbers are multiples of 2.

1.1 Proposition (Properties of divisibility)

1. The number 1 divides all integers.
2. $d \mid 0$ and $d \mid d$ for any integer $d \neq 0$.
3. If $d \mid m$ and $m \mid n$ then $d \mid n$.
4. If $d \mid m$ and $d \mid n$ then $d \mid (am + bn)$ for any integers a and b .

Proof. The first two statements follow immediately from the definition of divisibility. For (3) simply observe that if m/d and n/m are integers then so is $n/d = n/m \times m/d$. Similarly for (4), the number $(am + bn)/d = a(m/d) + b(n/d)$ is an integer when $d \mid m$ and $d \mid n$. ▽

Definition. For every real number x , the notation $\lfloor x \rfloor$ denotes the greatest integer $\leq x$. For example $\lfloor 3.14 \rfloor = 3$ and $\lfloor 2 \rfloor = 2$. Now with $n > 0$, define the *residue of m mod n* by $m \% n = m - \lfloor m/n \rfloor n$. Here the symbol (%) is read “mod”. For example $18 \% 5 = 3$

¹Copyrighted under a Creative Commons License

²Last Revision: 24-12-2006

and $18 \% 3 = 0$. Note that $m \% n$ is really the remainder upon dividing m by n and it lies in the range $0 \leq m \% n \leq n - 1$. In particular $m \% n = 0$ if and only if $n \mid m$.

Exercise. Find these residues.

1. $369 \% 5$
2. $24 \% 8$
3. $123456789 \% 10$
4. $7 \% 11$

1.2 Proposition One in every n consecutive integers is divisible by n .

Proof. Let m be the first integer and let $k = m \% n$. If $k = 0$ then $n \mid m$. Otherwise $1 \leq k \leq n - 1$ and our consecutive integers can be written

$$m = \lfloor m/n \rfloor n + k, \lfloor m/n \rfloor n + (k + 1), \lfloor m/n \rfloor n + (k + 2), \dots, \lfloor m/n \rfloor n + (k + n - 1)$$

with $k + n - 1 \geq n$. Then one of these numbers is $\lfloor m/n \rfloor n + n$, a multiple of n . ∇

Definition. The *greatest common divisor* of two integers m and n is the largest integer which divides both. This number is denoted by $\gcd(m, n)$. For example $\gcd(18, 24) = 6$ because 6 is the largest integer with the property $6 \mid 18$ and $6 \mid 24$.

Exercise. Find $\gcd(36, -48)$, $\gcd(24, 0)$, $\gcd(1, 99)$, $\gcd(100, 123)$.

1.3 The Euclidean Algorithm $\gcd(m, n) = \gcd(n, m \% n)$

Proof. It suffices to show that the two pairs $\{m, n\}$ and $\{n, m \% n\}$ have identical sets of common divisors. This is achieved entirely using Proposition 1.1.4 upon observing that, from its definition, $m \% n$ is a linear combination of m and n , and so is m of n and $m \% n$. ∇

Exercise. Use Euclidean Algorithm to compute $\gcd(m, n)$.

1. $m = 144, n = 456$
2. $m = 503, n = 999$
3. $m = 725, n = 1000$
4. $m = 12345, n = 67890$

1.4 Theorem $\gcd(m, n) = am + bn$ for some integers a and b .

Proof. Note that applying the Euclidean Algorithm successively will always terminate with zero as the last residue:

$$\gcd(m, n) = \gcd(n, m \% n) = \gcd(m \% n, n \% (m \% n)) = \dots = \gcd(d, 0)$$

in which case $\gcd(m, n) = d$. Since each integer in the pair is a linear combination of the previous pair of integers, we may by a finite number of steps express d as a linear combination of m and n . ∇

Remark. The algorithm involved in actually finding the integers a and b is called the Extended Euclidean Algorithm, the details of which will be discussed in Project 1 given at the end of this chapter.

1.5 Corollary Let L be the set of all integral linear combinations of m and n . Then

1. L is equal to the set of all multiples of $\gcd(m, n)$.
2. $\gcd(m, n)$ is the least positive element of L .
3. $\gcd(m, n) = 1$ if and only if $1 \in L$.
4. $\gcd(m, n) = 1$ if and only if L is the set of all integers.

Proof. All multiples of $\gcd(m, n)$ belong to L by Theorem 1.4. Conversely $\gcd(m, n)$ divides every element of L according to Proposition 1.1.4. This proves the first statement, from which follow the remaining three. ∇

1.6 Proposition (Properties of greatest common divisors)

1. If $d \mid m$ and $d \mid n$ then $d \mid \gcd(m, n)$.
2. If $d \mid \gcd(m, n)$ then $\gcd(m/d, n/d) = \gcd(m, n)/d$.
3. If $d \mid mn$ and $\gcd(d, m) = 1$ then $d \mid n$.
4. If $c \mid m$ and $d \mid m$ with $\gcd(c, d) = 1$ then $cd \mid m$.
5. If $\gcd(m, n) = 1$ and $\gcd(m', n) = 1$ then $\gcd(mm', n) = 1$.

Euclid’s Lemma

Proof. (1) This is a corollary of Theorem 1.4 and Proposition 1.1.4.

(2) By Corollary 1.5.2, $\gcd(m/d, n/d)$ is the least positive linear combination of m/d and n/d , which is $1/d$ times the least positive linear combination of m and n , that is $\gcd(m, n)/d$.

(3) By Theorem 1.4 if $\gcd(d, m) = 1$ then $1 = ad + bm$ for some integers a and b . Multiplying this last equation by n/d yields $n/d = an + b(mn/d)$, which is an integer if $d \mid mn$.

(4) Again $\gcd(c, d) = 1$ implies $1 = ac + bd$. This time multiply through by $m/(cd)$ to get $m/(cd) = a(m/d) + b(m/c)$, which is an integer if $c \mid m$ and $d \mid m$.

(5) Write $1 = am + bn$ and $1 = a'm' + b'n$ and multiply the two equations together:

$$1 = aa'mm' + (ab'm + a'bm' + bb'n)n$$

This displays 1 as a linear combination of mm' and n and hence $\gcd(mm', n) = 1$ by Corollary 1.5.3. ∇

1.7 Linear Equation Theorem The linear equation $mx + ny = c$ has a solution if and only if $d = \gcd(m, n) \mid c$, in which case all its solutions are given by $(x_0 - k\frac{n}{d}, y_0 + k\frac{m}{d})$ for any particular solution (x_0, y_0) and for any integer k .

Proof. The first part of the theorem is a restatement of Corollary 1.5.1. Now suppose we have a particular solution (x_0, y_0) and consider first the case $d = 1$. All solutions of the linear equation must lie on the line passing through (x_0, y_0) with a slope equal $-m/n$. Another point on this line will be given by $(x_0 - t, y_0 + tm/n)$ for any real number t . If the coordinates are to be integers then by Euclid’s Lemma we must have $t = kn$ for some integer k . Thus the general solution $(x_0 - kn, y_0 + km)$.

For the case $d > 1$ we replace our equation by $(m/d)x + (n/d)y = c/d$ without altering its solution set. But then Proposition 1.6.2 implies that $\gcd(m/d, n/d) = 1$ and therefore the general solution is $(x_0 - kn/d, y_0 + km/d)$. ∇

Exercise. Find all the solutions, if any, of these equations.

1. $5x + 8y = 1$
2. $12x + 25y = 3$

3. $24x + 18y = 6$
4. $25x + 65y = 40$

1.8 Corollary $\gcd(m, n) = 1$ if and only if the equation $mx + ny = 1$ has a solution.

Proof. This follows since $\gcd(m, n) \mid 1$ if and only if $\gcd(m, n) = 1$. ◻

Problem Set 1

1. Does 3 divide 250313? What is $250313 \% 3$?
2. The time is now 11 o'clock in the morning. What time will it be after 100 hours?
3. Find all integers n in the range $1 \leq n \leq 12$ such that $\gcd(n, 12) = 1$.
4. Compute $\gcd(12345, 54321)$.
5. Find a solution of $34x + 55y = 1$.
6. Find all the solutions of $25x + 65y = 270$.
7. I made two calls today via MobileCom, one call to another MobileCom line for 6 piasters per minute and another call to a FastLink number for 16 piasters per minute. The total charge was 90 piasters. For how long did I talk in each call?
8. Investigate true or false.
 - (a) If $d \mid m$ then $d \leq m$.
 - (b) If $m \mid n$ and $n \mid m$ then $m = n$.
 - (c) If $c \mid m$ and $d \mid n$ then $cd \mid mn$.
 - (d) If $d \mid mn$ then either $d \mid m$ or $d \mid n$.
 - (e) If $dn \mid mn$ then $d \mid m$.
9. Investigate true or false.
 - (a) $\gcd(m, n) > 0$
 - (b) $\gcd(m, n) = \gcd(m - n, n)$
 - (c) $\gcd(m, mn) = m$
 - (d) $\gcd(m, m + 1) = 1$
 - (e) $\gcd(m, m + 2) = 2$
10. Prove that if $k > 0$ then $\gcd(km, kn) = k \gcd(m, n)$.
11. Prove that $n^2 + n$ is even.
12. Prove that $n^2 + 2$ is not divisible by 4.
13. Prove that $n^2 - 1$ is a multiple of 8 when n is odd.
14. Prove $6 \mid (n^3 - n)$.
15. Prove $24 \mid (n^3 - n)$ if n is odd.
16. Prove $30 \mid (n^5 - n)$.

Project 1 Extended Euclidean Algorithm

The goal is to express the greatest common divisor of two integers as their linear combination, that is to write $\gcd(m, n) = am + bn$ for some integers a and b . We have seen how the Euclidean Algorithm is used to evaluate $\gcd(m, n)$. For example we find that $\gcd(216, 78) = 6$ as the last non-zero remainder in the following recursive steps.

$$\begin{aligned}
 216 &= 2(78) + 60 \\
 78 &= 1(60) + 18 \\
 60 &= 3(18) + 6 \\
 18 &= 3(6) + 0
 \end{aligned}$$

Now rewrite these equations in order to express each remainder as a linear combination of $m = 216$ and $n = 78$.

$$\begin{aligned}
 60 &= 1(216) - 2(78) \\
 18 &= 1(78) - 1(60) \\
 &= 1(78) - 1\{1(216) - 2(78)\} \\
 &= -1(216) + 3(78) \\
 6 &= 1(60) - 3(18) \\
 &= 1\{1(216) - 2(78)\} - 3\{-1(216) + 3(78)\} \\
 &= 4(216) - 11(78)
 \end{aligned}$$

We shall next simplify the appearance of the above algorithm by not writing the m and n in each row. For convenience we add two extra rows at the top, corresponding to the equations $216 = 1(216) + 0(78)$ and $78 = 0(216) + 1(78)$, in this order.

$$\begin{array}{rcc}
 216 & 1 & 0 \\
 78 & 0 & 1 \\
 60 & 1 & -2 \\
 18 & -1 & 3 \\
 6 & 4 & -11
 \end{array}$$

Recall that the last row gives the desired result $\gcd(216, 78) = 6 = 4(216) - 11(78)$.

If we label the first column, from the top down r_1, r_2, r_3, \dots then these numbers satisfy the recurrence relation given by $r_n = \lfloor r_n/r_{n+1} \rfloor r_{n+1} + r_{n+2}$, which means that row $(n+2)$ is obtained by subtracting $\lfloor r_n/r_{n+1} \rfloor$ times row $(n+1)$ from row n .

Exercise. Continue with Exercise 1.3 to find a and b such that $\gcd(m, n) = am + bn$.

Assignment. Repeat this exercise with $m = 180180$ and n equals the number obtained from the last six digits of your Philadelphia University Number. This is your personal 6-digit PUN, to be remembered and used again in subsequent projects.

2 Prime Numbers

Definition. A *prime* number is an integer $p > 1$ with no positive divisors except 1 and p itself. An integer $n > 1$ which is not a prime number is called *composite*. For example 13 and 17 are primes, but 21 is composite because $21 = 3 \cdot 7$. Throughout these notes we shall designate p to always denote a prime number.

Exercise. Find all prime numbers up to 100.

2.1 Proposition (Properties of primes)

1. Every integer greater than 1 has a prime divisor.
2. n is composite if and only if it has a prime divisor $\leq \sqrt{n}$.
3. $\gcd(p, n) = p$ if $p \mid n$, otherwise $\gcd(p, n) = 1$.
4. If $p \mid mn$ then either $p \mid m$ or $p \mid n$.
5. If $p \mid n_1 n_2 \cdots n_k$ then p divides one of n_1, n_2, \dots, n_k .

Proof. (1) Suppose, by induction, the statement is true up to $n - 1$. Either n is prime, and its own prime divisor, or else it has a divisor d satisfying $1 < d < n$. It follows that d has a prime divisor which is also a divisor of n by Proposition 1.1.3.

(2) For prime p there is clearly no prime divisor $\leq \sqrt{p}$. For composite $n = ab$ with $a, b > 1$ either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ must hold. Whichever is true, by (1) a or b has a prime divisor d , which satisfies $d \leq \sqrt{n}$ and $d \mid n$.

(3) The statement is obvious since 1 and p are the only divisors of p .

(4) If $p \nmid m$ then by (3) $\gcd(p, m) = 1$ and by Euclid's Lemma $p \mid n$.

(5) Repeated use of (4) establishes this claim. ∇

2.2 Theorem There are infinitely many prime numbers.

Proof. If there were only finitely many prime numbers, let N be the product of them all. Now by Proposition 2.1.1, one of these prime divisors of N must also divide $N + 1$, thus it would also divide $1 = (N + 1) - N$ according to Proposition 1.1.4. This is absurd because all primes are larger than 1. ∇

2.3 The Fundamental Theorem of Arithmetic Every integer greater than 1 is a product of prime numbers in a unique way up to reordering.

Proof. We use induction to show that such integer is a product of primes. Suppose this claim is true up to $n - 1$. By Proposition 2.1.1, n has a prime divisor, say $n = pn'$ with $n' < n$. It follows that n' is a product of primes and so is n .

To prove uniqueness we proceed by contradiction. Suppose we have two different multisets of primes p 's and q 's whose products both equal n . Equating these products and cancelling out all common terms will result in $p_1 p_2 \cdots p_j = q_1 q_2 \cdots q_k$ where none of the p 's equals any of the q 's. By Proposition 2.1.5, p_1 must divide one of the q 's, say q_i , implying that $p_1 = q_i$, a contradiction. ∇

Exercise. Factor the numbers 123, 400, 720, 7575 into primes.

2.4 Corollary Let m and n be factored into powers of distinct primes: $m = \prod p_i^{j_i}$ and $n = \prod p_i^{k_i}$, with $j_i, k_i \geq 0$. Then $\gcd(m, n) = \prod p_i^{e_i}$ where $e_i = \min\{j_i, k_i\}$.

Proof. By Theorem 2.3 a divisor of m must be of the form $d = \prod p_i^{e_i}$ with $e_i \leq j_i$. Similarly if $d \mid n$ then $e_i \leq k_i$ and so the greatest such d is the case $e_i = \min\{j_i, k_i\}$. ∇

Exercise. Find $\gcd(m, n)$.

1. $m = 2^2 \cdot 3 \cdot 5^3 \cdot 7^3, n = 2^5 \cdot 3^2 \cdot 5 \cdot 7^2$
2. $m = 2^3 \cdot 3^8 \cdot 5^4 \cdot 7^5, n = 3^7 \cdot 5^2 \cdot 7^2$
3. $m = 2^5 \cdot 5^7 \cdot 11^3, n = 3^7 \cdot 7^2 \cdot 13^9$
4. $m = 2^4 \cdot 5^2 \cdot 7 \cdot 11^3, n = 2^7 \cdot 3^2 \cdot 5^2 \cdot 11$

2.5 Conjectures (Unsolved problems concerning prime numbers)

1. There are infinitely many primes in the sequence $\{n^2 + 1\}$.
2. *Twin Primes.* There are infinitely many primes in the sequence $\{p + 2\}$.
3. *Mersenne Primes.* There are infinitely many primes in the sequence $\{2^p - 1\}$.
4. *Fermat Primes.* There are only finitely many primes in the sequence $\{2^{2^n} + 1\}$.
5. *Goldbach's Conjecture.* Every even number $n > 2$ is a sum of two primes.

2.6 Dirichlet’s Theorem on Primes in Arithmetic Progressions There are infinitely many primes in the sequence $\{an + b\}$ if and only if $\gcd(a, b) = 1$.

Proof for $a = 4$ and $b = 3$. First note that a prime $p > 2$ must have the form $4n + 1$ or $4n + 3$. Second, the product of two numbers in the form $4n + 1$ is again of the same form, hence a number in the form $4n + 3$ must have a prime divisor of the form $4n + 3$.

We claim that there are infinitely many primes in the sequence $\{4n + 3\}$. If it were not so, let N be the product of them all. As noted, one of these prime divisors of N must be a prime divisor of the number $4(N - 1) + 3$ hence it would also divide $1 = 4N - (4(N - 1) + 3)$ and this is a contradiction. ∇

2.7 The Prime Number Theorem Let $\pi(x)$ denote the number of primes up to x . For example $\pi(13) = |\{2, 3, 5, 7, 11, 13\}| = 6$ and $\pi(100) = 25$. Then

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\log x} = 1$$

and even more accurately, $\pi(x)$ can be estimated by $x/(\log x - 1)$ for large values of x .

No Proof. The proof is beyond the scope of elementary number theory. ∇

Exercise. Approximately how many prime numbers are there up to 10,000,000?

Problem Set 2

1. Factor the number 250313 into primes.
2. Find all the positive divisors of $300 = 2^2 \cdot 3 \cdot 5^2$.
3. How many positive integers divide the number $n = 2^4 \cdot 3^2 \cdot 5 \cdot 7^3$?
4. Find all pairs of twin primes up to 100.
5. Find all primes in the form $n^2 + 1$ up to 100.
6. Write the number 2006 as a sum of two primes in five different ways.
7. Find five Mersenne primes.
8. Find five Fermat primes.
9. Estimate the number of primes up to one million.
10. Estimate the number of primes among the ten-digit integers.
11. Investigate true or false.
 - (a) $n^2 + n + 41$ is prime for all $n \geq 0$.
 - (b) $n^2 - 81n + 1681$ is prime for all $n \geq 1$.
 - (c) If $p \mid n^2$ then $p^2 \mid n^2$.
 - (d) If $p \mid n^2$ then $p \mid n$.
 - (e) If $p \mid n^k$ then $p \mid n$.
12. The *least common multiple* of two integers is the smallest positive integer which is divisible by both. For example $\text{lcm}(4, 6) = 12$ because 12 is the smallest positive integer with the property $4 \mid 12$ and $6 \mid 12$.
 - (a) Use prime factorization to find a formula for $\text{lcm}(m, n)$.
 - (b) Find a relation between $\gcd(m, n)$ and $\text{lcm}(m, n)$.
 - (c) Illustrate your answers using $m = 600$ and $n = 630$.
13. Prove that if $d^2 \mid m^2$ then $d \mid m$.
14. Prove $\gcd(m^2, n^2) = \gcd(m, n)^2$.
15. Find all prime triplets, namely $p, p + 2, p + 4$, all of which are primes.
16. Prove that there are infinitely many primes in the sequence $\{6n + 5\}$.

Project 2 Fermat Factorization

If $n = x^2 - y^2$ then it factors to $n = (x + y)(x - y)$. This fact is the simple idea behind the method of Fermat Factorization. We seek a factor of n by calculating the numbers $y^2 = x^2 - n$ for each integer $x \geq \sqrt{n}$ until we find a perfect square. For example with $n = 4277$ we first calculate $\sqrt{4277} \approx 65.39$ so we start with $x = 66$.

$$\begin{aligned} 66^2 - 4277 &= 79 \\ 67^2 - 4277 &= 212 \\ 68^2 - 4277 &= 347 \\ 69^2 - 4277 &= 484 = 22^2 \end{aligned}$$

The result is $4277 = 69^2 - 22^2 = (69 + 22)(69 - 22) = 91 \cdot 47$.

Fermat Factorization always works when n is odd because if $n = ab$ with both a, b odd then $n = x^2 - y^2$ with $x = (a + b)/2$ and $y = (a - b)/2$. Moreover this shows that we should terminate the process when $x = (n + 1)/2$, in which case $n = n \cdot 1$ is a prime.

Exercise. Follow the above example with the numbers 2117, 16781, 65593, and 70027.

Assignment. With the help of Fermat Factorization try to factor into primes your personal 6-digit PUN from Project 1.

3 Congruences

Definition. Two integers a and b are *congruent modulo* $n > 0$ if $n \mid (a - b)$, in which case we write $a \equiv b \pmod{n}$. Equivalently we may define $a \equiv b \pmod{n}$ to mean $a \% n = b \% n$ and in particular $a \equiv a \% n \pmod{n}$. For example $13 \equiv 4 \pmod{3}$ and for arbitrary even numbers a and b we have $a \equiv b \equiv 0 \pmod{2}$.

3.1 Proposition (Properties of congruences)

1. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $a + c \equiv b + d \pmod{n}$.
2. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then $ac \equiv bd \pmod{n}$.
3. If $a \equiv b \pmod{n}$ then $f(a) \equiv f(b) \pmod{n}$ for any integral polynomial $f(x)$.
4. If $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ with $\gcd(m, n) = 1$ then $a \equiv b \pmod{mn}$.
5. If $ma \equiv mb \pmod{n}$ and $\gcd(m, n) = 1$ then $a \equiv b \pmod{n}$.

Proof. First note that $a \equiv b \pmod{n}$ holds if and only if $a = b + jn$ for some integer j . Now if both $a = b + jn$ and $c = d + kn$ then the sum $a + c = b + d + (j + k)n$ and the product $ac = bd + (bk + jd + jkn)n$ show why (1) and (2) are true.

For the remaining claims, (3) is a natural generalization of (1) and (2), whereas (4) follows directly from Proposition 1.6.4, and (5) from Euclid's Lemma. ∇

Definition. Congruence modulo n is an equivalence relation over the integers with n *congruence classes*, namely the classes of integers whose residues mod n are $0, 1, 2, \dots$, up to $n - 1$. A set of n numbers form a *complete residue system* modulo n if each comes from a different congruence class. For example a complete residue system modulo 7 can be $\{0, 1, 2, 3, 4, 5, 6\}$, $\{1, 2, 3, 4, 5, 6, 7\}$, or $\{0, 1, 2, 10, 11, 75, -1\}$, etc.

Exercise. Find a complete residue system modulo 7 with only even numbers.

3.2 Linear Congruence Theorem The congruence $mx \equiv c \pmod{n}$ has a solution if and only if $d = \gcd(m, n) \mid c$, in which case it has exactly d solutions modulo n given by $x \equiv x_0 + kn/d \pmod{n}$ for $k = 0, 1, 2, \dots, d - 1$ and for any particular solution x_0 .

Proof. The congruence is equivalent to the linear equation $mx = c + ny$ and the theorem is really a corollary of the Linear Equation Theorem. ∇

Exercise. Count how many solutions each congruence has, then find them.

1. $8x \equiv 5 \pmod{13}$
2. $35x \equiv 7 \pmod{49}$
3. $27x \equiv 1 \pmod{209}$
4. $6x \equiv 9 \pmod{1023}$

Definition. Two integers a and b are *inverses* of each other modulo n if $ab \equiv 1 \pmod{n}$. For example 3 and 5 are inverses modulo 7 since $3 \cdot 5 = 15 \equiv 1 \pmod{7}$. Similarly the congruence $5^2 \equiv 1 \pmod{12}$ implies that 5 is its own inverse modulo 12.

3.3 Modular Inverse Theorem The number a has an inverse modulo n if and only if $\gcd(a, n) = 1$, in which case its inverse, written $b = a^{-1}$, is unique modulo n .

Proof. Simply let $m = a$ and $c = 1$ in the Linear Congruence Theorem. ∇

Exercise. Find a^{-1} modulo n if it exists.

1. $a = 2, n = 7$
2. $a = -5, n = 8$
3. $a = 35, n = 42$
4. $a = 27, n = 209$

3.4 Chinese Remainder Theorem If $\gcd(m, n) = 1$ then the pair of congruences $x \equiv c \pmod{m}$ and $x \equiv d \pmod{n}$ have a unique common solution modulo mn .

Proof. All solutions of $x \equiv c \pmod{m}$ are of the form $c + mk$, which is a common solution if and only if $c + mk \equiv d \pmod{n}$, or $mk \equiv d - c \pmod{n}$. By the Linear Congruence Theorem there exists such an integer k since $\gcd(m, n) = 1 \mid (d - c)$.

Now any two solutions must satisfy $x_1 \equiv c \equiv x_2 \pmod{m}$ and $x_1 \equiv d \equiv x_2 \pmod{n}$ so that $x_1 \equiv x_2 \pmod{mn}$ by Proposition 3.1.4, proving uniqueness. ∇

Exercise. Find a common solution of $x \equiv 5 \pmod{8}$ and $x \equiv 7 \pmod{11}$.

Definition. The numbers m and n are *relatively prime* if $\gcd(m, n) = 1$. Three or more integers are *pairwise relatively prime* if they are relatively prime one to another. An example is 8, 11, and 15, where $\gcd(8, 11) = \gcd(8, 15) = \gcd(11, 15) = 1$.

3.5 Chinese Remainder Theorem (General) Suppose n_1, n_2, \dots, n_k are pairwise relatively prime. Then the system of congruences $x \equiv c_i \pmod{n_i}$ for $i = 1, 2, \dots, k$ has a unique solution modulo $N = n_1 n_2 \cdots n_k$. Explicitly the solution is given by

$$x \equiv \sum_{i=1}^k c_i \left(\frac{N}{n_i}\right) \left(\frac{N}{n_i}\right)^{-1} \pmod{N}$$

where each inverse is taken modulo n_i .

Proof. To check that the solution satisfies the system is trivial for $c_i \left(\frac{N}{n_i}\right) \left(\frac{N}{n_i}\right)^{-1} \equiv c_i \pmod{n_i}$ for each i . To see that this solution is unique is again by the use of Proposition 3.1.4, together with Proposition 1.6.5. ∇

Exercise. Find the smallest integer $x > 0$ satisfying the system of congruences.

1. $x \equiv 5 \pmod{8}, x \equiv 7 \pmod{11}$
2. $x \equiv 3 \pmod{4}, x \equiv 2 \pmod{5}, x \equiv 5 \pmod{7}$
3. $x \equiv 1 \pmod{9}, x \equiv 2 \pmod{10}, x \equiv 3 \pmod{11}$
4. $x \equiv 1 \pmod{2}, x \equiv 2 \pmod{3}, x \equiv 1 \pmod{5}, x \equiv 2 \pmod{7}$

3.6 Lemma If $a^2 \equiv 1 \pmod{p}$ then $a \equiv \pm 1 \pmod{p}$.

Proof. According to Proposition 2.1.4, if p divides $a^2 - 1 = (a+1)(a-1)$ then $p \mid (a+1)$ or $p \mid (a-1)$, which is equivalent to the statement of the lemma. ∇

3.7 Wilson's Theorem If p is prime then $(p-1)! \equiv -1 \pmod{p}$.

Proof. The Modular Inverse Theorem assures that each of the numbers $1, 2, \dots, p-1$ has an inverse modulo p , and by Lemma 3.6 none of them is self-inverse, except 1 and $p-1$. Hence $(p-1)!$ consists of the product of pairs of inverses modulo p , except 1 and $p-1$, which do not get paired up. This gives the desired congruence. ∇

Exercise. Compute $k! \% 13$ for $k = 11, 12, 13, 14$.

Problem Set 3

1. Find a complete residue system modulo 9 with only odd numbers.
2. Find a complete residue system modulo 5 with only prime numbers.
3. Find all the solutions of $12x \equiv 18 \pmod{54}$.
4. Find the inverse of 7 modulo 12.
5. Which integers a in the range $1 \leq a \leq 12$ have an inverse modulo 12?
6. Find the smallest integer $x > 1$ which satisfies all three congruences $x \equiv 1 \pmod{7}$ and $x \equiv 1 \pmod{11}$ and $x \equiv 1 \pmod{13}$.
7. Find complete solution to the system $x \equiv 2 \pmod{5}, x \equiv 1 \pmod{8}, x \equiv 7 \pmod{9}$, and $x \equiv -3 \pmod{11}$.
8. I have less than 3 dinars left in my MobileCom prepaid account. I could try to spend it all by sending local SMSs, for 3 piasters each, but then 1 piaster would be left. Or I could use it all on international SMSs, 7 piasters each, then 3 piasters would be left. Or MMSs, 13 piasters each, and 2 piasters would be left. How much credits exactly do I have?
9. Investigate true or false.
 - (a) If $a \equiv b \pmod{n}$ and $d \mid n$ then $a \equiv b \pmod{d}$.
 - (b) If $a \equiv b \pmod{n}$ then $\gcd(a, n) = \gcd(b, n)$.
 - (c) If $a \equiv b \pmod{n}$ then $ma \equiv mb \pmod{mn}$.
 - (d) If $ma \equiv mb \pmod{mn}$ then $a \equiv b \pmod{n}$.
 - (e) If $ma \equiv mb \pmod{n}$ then $a \equiv b \pmod{n}$.
10. Prove $37 \mid (35! - 1)$.
11. Prove $37 \mid (34! - 18)$.
12. Prove that if a is odd then $a^2 \equiv 1 \pmod{8}$.

13. Prove that if $p \equiv 1 \pmod{3}$ then $p \equiv 1 \pmod{6}$.
14. Prove that if $a^2 \equiv b^2 \pmod{p}$ then either $a \equiv b \pmod{p}$ or $a \equiv -b \pmod{p}$.
15. Prove that if $a \equiv b \pmod{m}$ and $a \equiv b \pmod{n}$ then $a \equiv b \pmod{\text{lcm}(m, n)}$.
16. Prove that the converse of Wilson's Theorem is also true.

Project 3 Divisibility Tests

A number n is divisible by 9 if and only if the sum of its digits is divisible by 9. For example a multiple of 9 is the number $1504296 = 9 \cdot 167144$ where the digit sum is $1 + 5 + 0 + 4 + 2 + 9 + 6 = 27$, again a multiple of 9. To see why this is true, let

$$n = a_n(10^n) + a_{n-1}(10^{n-1}) + \cdots + a_2(10^2) + a_1(10) + a_0$$

with $0 \leq a_i \leq 9$ for each term. This simply gives the decimal representation of n with digits, from right to left, $a_0, a_1, a_2, \dots, a_n$. Since $10 \equiv 1 \pmod{9}$, Proposition 3.1.3 turns the equation to the congruence $n \equiv a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 \pmod{9}$.

Similarly a $3k$ -digit number n is divisible by 7, 11, or 13 if and only if the alternating sum of the k consecutive 3-digit substrings of n is divisible by 7, 11, or 13, respectively. To illustrate this let $n = 007656103$, where the two leading zeros have been added to make the number of digits a multiple of 3. We have $007 - 656 + 103 = -546 = -2 \cdot 3 \cdot 7 \cdot 13$, meaning that n is divisible by 7 and 13 but not by 11.

Exercise. Prove this using the fact that $1000 \equiv -1 \pmod{7, 11, 13}$ and also prove that n is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

Exercise. Given an integer n , remove the right-most digit, say u , and denote what remains by t . Then n is divisible by 17 if and only if $t - 5u$ is, and by 19 if and only if $t + 2u$ is. Verify these facts using several examples and try to prove them.

Assignment. Make a summary of Divisibility Tests to determine when a number n is divisible by $d = 2, 3, \dots, 19$ and illustrate each test using your *full* 9-digit PUN as n . In the end try to factor n into primes.

4 Modular Exponentiation

4.1 Successive Squaring Algorithm An efficient method for computing $a^k \% n$ for large integer k is to first express k as the sum of powers of 2, then compute $a^2 \% n, a^4 \% n, a^8 \% n, \dots$ up to the highest exponent in those summands.

Exercise. Use the algorithm to compute these residues.

1. $3^{99} \% 20$
2. $25^{999} \% 9$
3. $47^{250} \% 100$
4. $99^{100} \% 101$

4.2 Lemma If $\text{gcd}(a, n) = 1$ then $\{r_1, r_2, \dots, r_n\}$ is a complete residue system modulo n if and only if $\{ar_1, ar_2, \dots, ar_n\}$ is also a complete residue system modulo n .

Proof. By Proposition 3.1.4, $ar_j \equiv ar_k \pmod{n}$ implies $r_j \equiv r_k \pmod{n}$ if $\gcd(a, n) = 1$, in which case $\{ar_1, ar_2, \dots, ar_n\}$ represents distinct congruence classes modulo n if and only if $\{r_1, r_2, \dots, r_n\}$ also represents distinct congruence classes modulo n . ∇

Exercise. Illustrate this lemma with $a = 4$ and $n = 9$.

4.3 Fermat's Little Theorem If $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. By Lemma 4.2 the numbers $0, a, 2a, \dots, (p-1)a$ form a complete residue system modulo p , hence their residues mod p are $0, 1, 2, \dots, p-1$, not necessarily in this order. Leaving out 0, we obtain the following congruence by multiplying those numbers.

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

Wilson's Theorem then reduces this to $-a^{p-1} \equiv -1 \pmod{p}$ and the desired result. ∇

Exercise. Use the theorem to compute these residues.

1. $8^{40} \% 41$
2. $8^{42} \% 41$
3. $8^{2345} \% 41$
4. $5^{495} \% 239$

Definition. The *Euler phi-function* $\phi(n)$ is the number of positive integers up to n which are relatively prime to n . For example $\phi(10) = 4$ and $\phi(11) = 10$.

Exercise. Evaluate $\phi(12), \phi(13), \phi(14), \phi(15)$.

Definition. A *reduced residue system* modulo n is a subset of a complete residue system modulo n consisting of the $\phi(n)$ numbers relatively prime to n . For example $\{1, 2, 4, 5, 7, 8\}$ is a reduced residue system modulo 9.

Exercise. Find a reduced residue system modulo 10, 11, 12, 13.

4.4 Lemma If $\gcd(a, n) = 1$ then $\{r_1, r_2, \dots, r_{\phi(n)}\}$ is a reduced residue system modulo n if and only if $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$ is also a reduced residue system modulo n .

Proof. As in the proof of Lemma 4.2, either both sets represent distinct congruence classes or neither does. To finish the proof we need to show that $\gcd(ar_i, n) = 1$ if and only if $\gcd(r_i, n) = 1$, but this follows from Proposition 1.8.4 since $\gcd(a, n) = 1$. ∇

Exercise. Illustrate this lemma with $a = 4$ and $n = 9$.

4.5 Euler's Theorem If $\gcd(a, n) = 1$ then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. If $\gcd(a, n) = 1$ then by Lemma 4.4 we may choose a pair of reduced residue systems modulo n in the form $\{r_1, r_2, \dots, r_{\phi(n)}\}$ and $\{ar_1, ar_2, \dots, ar_{\phi(n)}\}$. Multiplying all the elements in each set yields the congruence

$$a^{\phi(n)} \cdot r_1 \cdot r_2 \cdots r_{\phi(n)} \equiv r_1 \cdot r_2 \cdots r_{\phi(n)} \pmod{n}$$

Since each element r_i in the set is relatively prime to n , Proposition 3.1.4 completes the proof by cancelling the common terms off both sides of the congruence. ∇

Exercise. Compute $7^{26} \% 10$ using Euler's Theorem.

Remark. As a computational corollary, when $\gcd(a, n) = 1$, the computation of $a^k \% n$ can be reduced by first replacing a by $a \% n$ and k by $k \% \phi(n)$. Euler's Theorem is not true, however, when $\gcd(a, n) \neq 1$. Nevertheless for small n we can find a similar reduction once we observe the periodicity of the sequence $a \% n, a^2 \% n, a^3 \% n, \dots$

Exercise. Compute the following residues.

1. $2^{26} \% 10$
2. $50^{345} \% 12$
3. $11^{123} \% 32$
4. $77^{3456} \% 900$

4.6 Theorem If $\gcd(m, n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$.

Proof. Let M, N , and MN be reduced residue systems modulo m, n , and mn , respectively. To complete the proof we shall provide a one-to-one correspondence between $M \times N$ and MN , thereby showing that $\phi(mn) = |MN| = |M \times N| = \phi(m)\phi(n)$.

For each $a \in MN$ we have $\gcd(a, mn) = 1$, thus $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$. Since M and N are reduced residue systems, there exists a unique pair $(c, d) \in M \times N$ such that $a \equiv c \pmod{m}$ and $a \equiv d \pmod{n}$. Conversely given a pair of congruences $x \equiv c \pmod{m}$ and $x \equiv d \pmod{n}$ with $(c, d) \in M \times N$, by Chinese Remainder Theorem and Proposition 1.6.5, $x = a$ is the unique element in MN which solves the system. This establishes the one-to-one correspondence between the two sets. ∇

4.7 Proposition (Evaluation of Euler phi-function)

1. $\phi(p) = p - 1$
2. $\phi(p^k) = p^k - p^{k-1}$
3. If $n = \prod p_i^{k_i}$ then $\phi(n) = \prod p_i^{k_i-1}(p_i - 1) = n \prod \left(1 - \frac{1}{p_i}\right)$.

Proof. The claim (1) is trivial. In (2) $\phi(p^k)$ is the number of integers from 1 to p^k which are relatively prime to p^k . Since p is the only prime divisor of p^k , this number is p^k minus the number of multiples of p , which are $p, 2p, 3p, \dots, (p^{k-1})p$. Thus $\phi(p^k) = p^k - p^{k-1}$. And finally (3) follows directly from (2) and Theorem 4.6. ∇

Exercise. Evaluate $\phi(61), \phi(62), \phi(63), \phi(64)$.

4.8 A Generalization of Euler's Theorem Let a and n be arbitrary positive integers. Set $n_0 = n$ and $d_0 = \gcd(a, n)$ then for $i \geq 1$ we define n_i and d_i recursively by $n_i = n_{i-1}/d_{i-1}$ and $d_i = \gcd(a, n_i)$. If k is the smallest integer for which $d_k = 1$ then

$$a^{\phi(n_k)+k} \equiv a^k \pmod{n}$$

in which Euler's Theorem coincides with the case $k = 0$.

Proof. We claim that the following statements are all equivalent, so that we are done since the very last one is true by Euler's Theorem.

- $a^{\phi(n_k)+k} \equiv a^k \pmod{n}$
- $a^{\phi(n_k)+k}/d_0 \equiv a^k/d_0 \pmod{n_1}$

- $a^{\phi(n_k)+k-1} \equiv a^{k-1} \pmod{n_1}$
- $a^{\phi(n_k)+k-1}/d_1 \equiv a^{k-1}/d_1 \pmod{n_2}$
- $a^{\phi(n_k)+k-2} \equiv a^{k-2} \pmod{n_2}$
- \vdots
- $a^{\phi(n_k)+1}/d_{k-1} \equiv a/d_{k-1} \pmod{n_k}$
- $a^{\phi(n_k)} \equiv 1 \pmod{n_k}$

To justify the equivalence, in each alternating step down the list we divide through the congruence including the modulus n_i by d_i to obtain the next modulus n_{i+1} . Immediately following this we divide the congruence, without the modulus, by a/d_i . This is allowed by Proposition 3.1.5 as $d_i = \gcd(a, n_i)$ implies $\gcd(a/d_i, n_{i+1}) = 1$ by Proposition 1.6.2. ∇

Exercise. Apply this theorem to compute $126^{9875} \% 432$.

4.9 Modular Root Extraction If both $\gcd(a, n) = 1$ and $\gcd(e, \phi(n)) = 1$ then the congruence $x^e \equiv a \pmod{n}$ has a unique root $x \equiv a^d \pmod{n}$ where $d \equiv e^{-1} \pmod{\phi(n)}$.

Proof. We may write $de = 1 + h\phi(n)$ for some integer h . Now raise to the power d both sides of the congruence $x^e \equiv a \pmod{n}$ to obtain

$$a^d \equiv x^{de} = x^{1+h\phi(n)} = x(x^{\phi(n)})^h \equiv x \pmod{n}$$

using Euler's Theorem. ∇

Exercise. Solve for x .

1. $x^7 \equiv 12 \pmod{13}$
2. $x^{13} \equiv 5 \pmod{32}$
3. $x^{121} \equiv 30 \pmod{899}$
4. $x^{239} \equiv 23 \pmod{2005}$

Problem Set 4

1. Find a reduced residue system modulo 24.
2. Find a reduced residue system modulo 15 with only odd numbers.
3. Evaluate $\phi(250313)$.
4. Find all positive integers n satisfying $\phi(n) = 4$.
5. Compute $5^{1434} \% 307$.
6. Compute $25^{1434} \% 309$.
7. What will be the right-most digit if we compute 1234^{5678} ?
8. Find the two right-most digits upon computing 123^{45678} .
9. Solve the congruence $x^{39} \equiv 5 \pmod{121}$.
10. Investigate true or false.
 - (a) $2^{6600} \equiv 1 \pmod{6601}$ hence the number 6601 must be a prime.
 - (b) $2^{1762} \equiv 742 \pmod{1763}$ hence 1763 cannot be a prime number.
 - (c) If $a \equiv b \pmod{n}$ then $a^k \equiv b^k \pmod{n}$.
 - (d) If $j \equiv k \pmod{n}$ then $a^j \equiv a^k \pmod{n}$.
11. Prove that Fermat's Little Theorem is equivalent to the following statement:
 $a^p \equiv a \pmod{p}$ for any integer a .

12. Prove that if $a^k \equiv 1 \pmod{n}$ for some $k > 0$ then $\gcd(a, n) = 1$.
13. Another property of $\phi(n)$ is that $\sum \phi(d) = n$ where the sum is taken over all the positive integers d which divide n . Verify this property for $n = 24$ and $n = 30$.
14. Prove that $\phi(2n) = 2\phi(n)$ if n is even and $\phi(2n) = \phi(n)$ if n is odd.
15. Prove that if $d \mid n$ then $\phi(d) \mid \phi(n)$.
16. Prove that $\phi(n)$ is even for all $n > 2$.

Project 4 The RSA Cryptosystem

Sensitive messages, when transferred over the internet, need to be encrypted, that is changed into a secret code in such a way that only the intended receiver who has the secret key is able to decrypt it. It is common that alphabetical characters are converted to their numerical ASCII equivalents before they are encrypted, hence the coded message will look like integer strings. The RSA Algorithm is an encryption-decryption process which is widely employed today.

Alia has a number $n = pq$ where p and q are very large distinct primes, over a hundred digits each. She computes $\phi(n) = \phi(pq) = (p-1)(q-1)$ and picks a number e relatively prime to $\phi(n)$ and another number $d \equiv e^{-1} \pmod{\phi(n)}$, found via the Euclidean Algorithm. She gives to Bob the pair (n, e) and keeps the rest secret. Then whenever Bob wants to send a message (integer) $m < n$ to Alia, he encrypts it to $s = m^e \% n$. Upon receiving s , Alia uses Theorem 4.9 to retrieve the message by computing $m = s^d \% n$.

Now if a bad guy intercepts the secret message s , together with e and n , he will yet have to find the factors p and q in order to compute $\phi(n)$. Woe to him, factoring a large integer the size of pq will take a lifetime on the best computers of today.

Assignment. Suppose it is known that $e = 3989$ and $n = 999697$. Using your 6-digit PUN as m , find the encrypted message s . Then try to break this code, perhaps using Fermat Factorization, and verify that you do indeed get m back.

Exercise. Suppose the encrypted message s is not relatively prime to n . Even though this is highly improbable since n has only two prime divisors, show that by Theorem 4.8, the decryption algorithm will anyhow return the correct message m .

5 Primitive Roots

Definition. Suppose a and n are relatively prime. The *order* of a modulo n is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$. We denote this quantity by $|a|_n$ or simply $|a|$ when there is no ambiguity. For example $|2|_7 = 3$ because $k = 3$ is the smallest positive solution of the congruence $2^k \equiv 1 \pmod{7}$. We reiterate that $|a|_n$ implicitly assumes that $\gcd(a, n) = 1$, hence we have $|a|_n \leq \phi(n)$ by Euler's Theorem.

Exercise. Find $|3|_7, |3|_{10}, |5|_{12}, |7|_{24}$.

5.1 Proposition (Properties of orders)

1. If $a \equiv b \pmod{n}$ then $|a|_n = |b|_n$.
2. $a^k \equiv 1 \pmod{n}$ if and only if $|a|_n \mid k$. In particular $|a|_n \mid \phi(n)$.
3. $a^j \equiv a^k \pmod{n}$ if and only if $j \equiv k \pmod{|a|_n}$.

4. $|a^k| = |a|$ if and only if $\gcd(k, |a|) = 1$.
5. If $\gcd(|a|, |b|) = 1$ then $|ab| = |a| |b|$.

Proof. (1) It is clear that the definition of order extends to congruence classes.

(2) Let $j = \lfloor k/|a|_n \rfloor$ so that we may write $k = j|a|_n + k \% |a|_n$. Then

$$a^k = (a^{|a|_n})^j \cdot a^{k \% |a|_n} \equiv a^{k \% |a|_n} \pmod{n}$$

and with the fact $k \% |a|_n < |a|_n$, the congruence $a^k \equiv 1 \pmod{n}$ holds if and only if $k \% |a|_n = 0$, equivalently $|a|_n \mid k$.

(3) The congruence $a^j \equiv a^k \pmod{n}$ is equivalent to $a^{j-k} \equiv 1 \pmod{n}$ and the result follows from (2).

(4) Observe that the following congruence

$$a^{jk} = (a^j)^k = (a^k)^j \equiv 1 \pmod{n}$$

is true if we let $j = |a|$, in which case $|a^k| \mid |a|$ by (2). It is also true with $j = |a^k|$ and similarly $|a| \mid k|a^k|$. If $\gcd(k, |a|) = 1$ then by Euclid's Lemma $|a| \mid |a^k|$ and so $|a^k| = |a|$. Conversely if $\gcd(k, |a|) = d > 1$, since the congruence holds for $j = |a|/d$, we have $|a^k| \leq |a|/d < |a|$.

(5) Suppose $\gcd(|a|, |b|) = 1$. Again we have the following congruence.

$$a^{|b||ab|} = a^{|b||ab|} (b^{|b|})^{|ab|} = (ab)^{|ab||b|} \equiv 1 \pmod{n}$$

Hence by (2) $|a| \mid |b||ab|$ and in turn, by Euclid's Lemma $|a| \mid |ab|$. Now by symmetry $|b| \mid |ab|$ and so $|a| |b| \mid |ab|$ by Proposition 1.6.4. It is clear, however, that $|ab| \leq |a| |b|$ so it follows that $|ab| = |a| |b|$. \square

Definition. An integer g is called a *primitive root* modulo n if $|g|_n = \phi(n)$. For example 3 is a primitive root modulo 7 because $|3|_7 = 6 = \phi(7)$.

Exercise. Find all the primitive roots modulo 6, 7, 8, 9, if any.

5.2 Proposition (Properties of primitive roots)

1. g is a primitive root modulo n if and only if $\{g, g^2, g^3, \dots, g^{\phi(n)}\}$ is a reduced residue system modulo n .
2. g is a primitive root modulo n if and only if the congruence $g^x \equiv c \pmod{n}$ has a solution for every integer c relatively prime to n .
3. If g is a primitive root modulo n then so is g^k if and only if $\gcd(k, \phi(n)) = 1$.
4. If any exists, there are exactly $\phi(\phi(n))$ primitive roots modulo n .

Proof. Let $G = \{g, g^2, g^3, \dots, g^{\phi(n)}\}$.

(1) If g is a primitive root then clearly each element in G is relatively prime to n . We show now that they represent distinct congruence classes, for if $g^j \equiv g^k \pmod{n}$ then by Proposition 5.1.3, $\phi(n) \mid (j - k)$. But this relation is not possible since $|j - k| < \phi(n)$ unless $j = k$. It follows that G is a reduced residue system modulo n . Conversely if g is not a primitive root then $g^k \equiv 1 \pmod{n}$ with $k < \phi(n)$ and G is not a reduced residue system for then $g^{k+1} \equiv g \pmod{n}$ where both $g^{k+1}, g \in G$.

(2) Equivalent to (1), G is a reduced residue system modulo n if and only if it represents all congruence classes of c with $\gcd(c, n) = 1$.

(3) This statement is a special case of Proposition 5.1.4.

(4) Exactly $\phi(\phi(n))$ elements $g^k \in G$ satisfy $\gcd(k, \phi(n)) = 1$ and by (3) these and only these are primitive roots modulo n . ∇

5.3 Theorem The number of solutions of $f(x) \equiv 0 \pmod{p}$ is at most the degree of f .

Proof. For a linear congruence, $ax + b \equiv 0 \pmod{p}$ has a unique solution according to the Linear Congruence Theorem since $\gcd(a, p) = 1$ and so the theorem is true.

By way of induction, assume the claim is true for polynomials of degree up to $n - 1$. Let $f(x)$ be a polynomial with leading term ax^n and with $p \nmid a$. If $f(x)$ has less than n roots then there is nothing to prove, else let r_1, r_2, \dots, r_n be distinct roots of $f(x)$ modulo p and let

$$g(x) = f(x) - a(x - r_1)(x - r_2) \cdots (x - r_n)$$

Note that the degree of $g(x)$ is less than n , and yet it has the same n roots of $f(x)$. By induction hypothesis this is impossible unless $g(x)$ is the zero polynomial \pmod{p} , so

$$f(x) \equiv a(x - r_1)(x - r_2) \cdots (x - r_n) \pmod{p}$$

and by Proposition 2.1.5 $f(x) \equiv 0 \pmod{p}$ if and only if $x \equiv r_i \pmod{p}$ for one of these roots. Thus $f(x)$ has only these n roots modulo p . ∇

5.4 Corollary If $d \mid (p - 1)$ then the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

Proof. Suppose $dk = p - 1$ so that we have the following polynomial identity.

$$x^{p-1} - 1 = (x^d - 1)((x^d)^{k-1} + (x^d)^{k-2} + \cdots + x^d + 1)$$

By Fermat's Little Theorem the left-hand side has exactly $p - 1$ roots modulo p . Since p is prime, these roots must come from those of the two polynomials on the right, which by Theorem 5.3 have at most d and $d(k - 1) = p - 1 - d$ roots, respectively. The only way this can happen is if their roots are exactly d and $p - 1 - d$. ∇

5.5 Theorem There are exactly $\phi(p - 1)$ primitive roots modulo every prime p .

Proof. In view of Proposition 5.2.4, it suffices to show that there is at least one primitive root modulo p .

Let $p - 1 = \prod q_i^{e_i}$ where the q 's are distinct primes and $e_i \geq 1$. By Corollary 5.4 there are exactly $q_1^{e_1}$ integer solutions of $x^{q_1^{e_1}} \equiv 1 \pmod{p}$, all of which have orders a power of q_1 according to Proposition 5.1.2. Similarly, however, $q_1^{e_1 - 1}$ of these integers satisfy the congruence $x^{q_1^{e_1 - 1}} \equiv 1 \pmod{p}$ hence their orders are no more than $q_1^{e_1 - 1}$. It follows that there exist $q_1^{e_1} - q_1^{e_1 - 1}$ integers of order $q_1^{e_1}$. By symmetry we have an integer of order $q_i^{e_i}$ for each of the distinct prime factors of $p - 1$. And the product of these integers, by Proposition 5.1.5, is of order $p - 1$, that is a primitive root. ∇

Exercise. How many are primitive roots modulo 5? 7? 11? 89?

5.6 Primitive Root Theorem Primitive roots exist only modulo $1, 2, 4, p^k$, or $2p^k$ for any prime $p > 2$ and $k > 0$.

No Proof. The proof is set aside as an independent assignment. ∇

Exercise. Is there a primitive root modulo 4? 8? 25? 50? 100? How many?

5.7 Artin’s Conjecture The number 2 is a primitive root for infinitely many primes.

5.8 Discrete Logarithm Problem The congruence $a^x \equiv b \pmod{p}$ with $p \nmid ab$ can be solved by writing a and b as powers of a primitive root g modulo p .

Exercise. Solve these mod-13 congruences using $g = 2$ with the help of the given table.

1. $4^x \equiv 10 \pmod{13}$
2. $5^x \equiv 9 \pmod{13}$
3. $2 \cdot 7^x \equiv 3 \pmod{13}$
4. $5 \cdot 8^x \equiv 11 \pmod{13}$

k	1	2	3	4	5	6	7	8	9	10	11	12
$2^k \pmod{13}$	2	4	8	3	6	12	11	9	5	10	7	1

Exercise. Use this table, in a similar way, to solve again Exercises 3.2.1 and 4.9.1.

Problem Set 5

1. Find the order of 4 modulo 25.
2. Is 5 a primitive root modulo 29?
3. Find all the primitive roots modulo 10.
4. Suppose $|a| = 6$. Find $|a^k|$ for $k = 2, 3, 4, 5, 6$.
5. One of the primitive roots modulo 11 is 2. Find the rest.
6. Is there a primitive root modulo 250313?
7. How many primitive roots are there modulo 1250?
8. Find three primes modulo which 2 is not a primitive root.
9. Solve the congruence $10 \cdot 6^x \equiv 12 \pmod{13}$.
10. Investigate true or false.

- (a) $|-a| = |a|$.
- (b) If $|a|_n = |b|_n$ then $a \equiv b \pmod{n}$.
- (c) If $a^j \equiv a^k \pmod{n}$ then $j \equiv k \pmod{n}$.
- (d) $a^k \equiv 1 \pmod{n}$ is not possible if $\gcd(a, n) \neq 1$.

11. Prove that if $|a|_n = n - 1$ then n must be a prime.
12. Prove that modular inverses have equal orders.
13. Prove that if g is a primitive root modulo $p > 2$ then $g^{(p-1)/2} \equiv -1 \pmod{p}$.
14. Prove that 4 is not a primitive root modulo any prime.
15. Prove that the product of two primitive roots modulo $p > 2$ is not a primitive root.
16. Prove that if $p \equiv 1 \pmod{4}$ then g is a primitive root modulo p if and only if $-g$ is too.

Project 5 Secret Key Exchange

For cryptological purposes, Alia and Bob need to establish a common secret key. However, the only available means of communication between them is the telephone, which they know is being tapped by the enemy. They resort to the Diffie-Hellman Key Exchange protocol as follows.

Alia chooses a large prime p , a primitive root g , and a positive integer $m < p$. She gives to Bob, over the non-secure telephone line, the numbers p , g , and $g^m \% p$ but keeps m secret. In turn Bob selects a secret number n and gives to Alia $g^n \% p$. They agree that their common secret key is $g^{mn} \% p$, which, employing Successive Squaring Algorithm, Alia obtains from $(g^n)^m \% p$ and Bob, independently, from $(g^m)^n \% p$.

If the enemy gathers this information (but not m and n for they are not transmitted across) they will have to solve the congruence $g^x \equiv a \pmod{p}$ where $a = g^m \% p$ or similarly $a = g^n \% p$ in order to capture the secret key. But the fact is, there is no efficient algorithm known to solve this Discrete Logarithm Problem, and for large p the problem is computationally infeasible.

Assignment. Illustrate the above idea with $p = 313$, $g = 10$, $m = 97$, and n is the residue mod p of your PUN. After that pretend you knew neither m nor n and try to find another way to retrieve the secret key $g^{mn} \% p$.

Exercise. Will this idea work if g is not a primitive root modulo p ? Think about it.

6 Quadratic Residues

Definition. A number a which is relatively prime to n is a *quadratic residue* modulo n if the congruence $x^2 \equiv a \pmod{n}$ has a solution. If it has no solution then a is called a *quadratic non-residue* modulo n . For example 19 is a quadratic residue modulo 5 since $19 \equiv 2^2 \pmod{5}$ whereas 7 is a non-residue because $x^2 \equiv 7 \pmod{5}$ has no solution.

Exercise. Find all the quadratic residues and non-residues modulo 5.

Definition. Let p be an odd prime. We define the so-called *Legendre symbol* as follows.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \\ 0 & \text{if } p \mid a \end{cases}$$

For example we have shown that $\left(\frac{19}{5}\right) = 1$ and $\left(\frac{7}{5}\right) = -1$. Henceforth the number p in the Legendre symbol $\left(\frac{a}{p}\right)$ is understood an odd prime, that is a prime larger than 2.

6.1 Proposition (Properties of the Legendre symbol)

1. $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b \pmod{p}$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$
3. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$

Euler's Criterion

Proof. It is clear that the definition of a quadratic residue extends to congruence classes, thus (1). Next we fix a primitive root g modulo p and claim that g^k is a quadratic residue if and only if k is even. Sufficiency is clear since $g^k = (g^{k/2})^2$ when k is even. For necessity observe that $g^j \equiv g^k \pmod{p}$ implies $2 \mid (p-1) \mid (j-k)$ by Proposition 5.1.3 and so j and k must be of the same parity. In particular if g^k is congruent to a square modulo p then k must be even.

By Proposition 5.2.2 we may assume $a = g^j$ and $b = g^k$. Now $ab = g^{j+k}$ is a quadratic residue if and only if $j+k$ is even, that is both j and k even or both odd. This is concisely expressed in (2).

Finally for the last claim, $\left(\frac{a}{p}\right) = 1$ if and only if $a = g^j$ with j even. But then $(g^j)^{(p-1)/2} = (g^{j/2})^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem. Conversely if j is odd, then $j - 1$ is even and similarly $(g^j)^{(p-1)/2} = (g^{j-1}g)^{(p-1)/2} \equiv g^{(p-1)/2} \pmod{p}$. However g being a primitive root implies that this last congruence reduces not to 1, but to $-1 \pmod{p}$ by Lemma 3.6. \square

6.2 Corollary $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

Proof. The two numbers are congruent modulo p by Euler's Criterion. However, since each is ± 1 and $p > 2$, this relation is possible only when both are equal. \square

Exercise. Is a a quadratic residue modulo p ? Use different ways to answer.

1. $a = -28, p = 5$
2. $a = 48, p = 7$
3. $a = -35, p = 11$
4. $a = 54, p = 13$

6.3 Gauss' Lemma If $p \nmid a$ then $\left(\frac{a}{p}\right) = (-1)^n$ where n is the number of integers in the set $\{a, 2a, 3a, \dots, \frac{p-1}{2}a\}$ whose residues mod p are larger than $p/2$.

Proof. Let A denote the set in the above statement. Replace each $x > p/2$ in the set $\{1, 2, \dots, p-1\}$ by $x - p$ to obtain another reduced residue system modulo p , call it $S = \{\pm 1, \pm 2, \dots, \pm \frac{p-1}{2}\}$. Hence n is the number of negative integers in S which are congruent modulo p to some elements in A .

We claim that for each pair of elements in A , if $ja \equiv \pm ka \pmod{p}$ then $j = k$. This is true because $p \nmid a$ so that the congruence can be written $j \equiv \pm k \pmod{p}$ with $j, \pm k \in \{1, 2, \dots, \frac{p-1}{2}\} \subseteq S$, and S being a reduced residue system forces $j = k$. This implies that, modulo p , the elements of A are reordering of the numbers $1, 2, \dots, \frac{p-1}{2}$, only that n of them have a negative sign:

$$a \cdot 2a \cdot 3a \cdots \frac{p-1}{2} a \equiv (-1)^n \cdot 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \pmod{p}$$

Cancel out the common terms since they are relatively prime to p and we have $a^{(p-1)/2} \equiv (-1)^n \pmod{p}$. Now apply Euler's Criterion to obtain the desired result. \square

Exercise. Illustrate Gauss' Lemma with $a = 5$ and $p = 11$.

6.4 Eisenstein's Lemma If $\gcd(a, 2p) = 1$ then $\left(\frac{a}{p}\right) = (-1)^m$ where $m = \sum_{k=1}^{(p-1)/2} [ka/p]$.

Proof. Our goal is to show that m is of the same parity as the number n in Gauss' Lemma, thereby making the two lemmas equivalent.

By definition $ka = [ka/p]p + ka \% p$ where, as in the proof of Gauss' Lemma, the numbers $ka \% p$, for $k = 1, 2, \dots, \frac{p-1}{2}$ are congruent modulo p , perhaps not in this order, to $1, 2, \dots, \frac{p-1}{2}$ but exactly n of them should have a negative sign. Denote by r 's those which should have been negatives and the rest by s 's so that

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} [ka/p]p + \sum_{i=1}^n p - r_i + \sum_{j=1}^{\frac{p-1}{2}-n} s_j$$

On the other hand we also have $\sum_{k=1}^{(p-1)/2} k = \sum_{i=1}^n r_i + \sum_{j=1}^{(p-1)/2-n} s_j$ and subtracting this from the last equation yields

$$(a-1) \sum_{k=1}^{\frac{p-1}{2}} k = \sum_{k=1}^{\frac{p-1}{2}} [ka/p]p + \sum_{i=1}^n p - 2 \sum_{i=1}^n r_i$$

Since $a \equiv p \equiv 1 \pmod{2}$, this in turn gives the congruence $0 \equiv \sum_{k=1}^{(p-1)/2} [ka/p] + n - 0 \pmod{2}$, that is $m \equiv n \pmod{2}$ as sought. ∇

Exercise. Illustrate Eisenstein’s Lemma with $a = 5$ and $p = 11$.

6.5 Corollary $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Proof. In the previous proof, substitute $a = 2$ in the last displayed equation to obtain $\sum_{k=1}^{(p-1)/2} k \equiv \sum_{k=1}^{(p-1)/2} [2k/p] + n - 0 \pmod{2}$. But each term $[2k/p] = 0$ because $2k < p$, whereas the left-hand side of the congruence is $\frac{1}{2} \left(\frac{p-1}{2}\right) \left(\frac{p+1}{2}\right) = \frac{p^2-1}{8}$ and the result then follows by Gauss’ Lemma. ∇

6.6 The Law of Quadratic Reciprocity If p and q are distinct odd primes then

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

In other words, $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$ if p or $q \equiv 1 \pmod{4}$ and $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ if $p \equiv q \equiv 3 \pmod{4}$.

Proof. Let $P = \{x \mid 1 \leq x \leq \frac{p-1}{2}\}$ and $Q = \{y \mid 1 \leq y \leq \frac{q-1}{2}\}$. Then $P \times Q$ contains $\left(\frac{p-1}{2}\right) \left(\frac{q-1}{2}\right)$ elements which can be partitioned into two subsets

$$S_1 = \{(x, y) \in P \times Q \mid py < qx\} \quad \text{and} \quad S_2 = \{(x, y) \in P \times Q \mid py > qx\}$$

Note that $py = qx$ is not possible as $p \nmid qx$. For each $x \in P$ we have $(x, y) \in S_1$ if and only if $1 \leq y \leq [qx/p]$, hence

$$|S_1| = \sum_{x=1}^{(p-1)/2} [qx/p] \quad \text{and similarly} \quad |S_2| = \sum_{y=1}^{(q-1)/2} [py/q]$$

Now raising -1 to the power $|P \times Q| = |S_1| + |S_2|$ yields

$$(-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} = (-1)^{\sum_{x=1}^{(p-1)/2} [qx/p]} \cdot (-1)^{\sum_{y=1}^{(q-1)/2} [py/q]}$$

and according to Eisenstein’s Lemma, the right-hand side of this is $\left(\frac{q}{p}\right) \left(\frac{p}{q}\right)$. ∇

Exercise. Evaluate the Legendre symbol $\left(\frac{a}{p}\right)$.

1. $a = 37, p = 83$
2. $a = 71, p = 103$
3. $a = -69, p = 127$
4. $a = 816, p = 239$

Definition. Let $P = p_1 p_2 \cdots p_k$ be the product of odd prime numbers, not necessarily distinct. Define the *Jacobi symbol*

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right)$$

and for convenience also let $\left(\frac{a}{1}\right) = 1$. For example $\left(\frac{14}{825}\right) = \left(\frac{14}{3}\right) \left(\frac{14}{5}\right) \left(\frac{14}{5}\right) \left(\frac{14}{11}\right)$. In the case $k = 1$, Jacobi symbol is really Legendre symbol. Moreover if $\gcd(a, P) = 1$ then the value of $\left(\frac{a}{P}\right)$ is ± 1 , and 0 otherwise. It is also true that if $\left(\frac{a}{P}\right) = -1$ then a is a quadratic non-residue modulo P , but the converse is not necessarily true.

Exercise. Is 14 a quadratic residue modulo 825?

6.7 Proposition (Properties of the Jacobi symbol)

1. $\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$ if $a \equiv b \pmod{P}$
2. $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right) \left(\frac{b}{P}\right)$
3. $\left(\frac{a}{PQ}\right) = \left(\frac{a}{P}\right) \left(\frac{a}{Q}\right)$

Proof. The congruence $a \equiv b \pmod{P = p_1 p_2 \cdots p_k}$ implies $a \equiv b \pmod{p_i}$ for each prime p_i . Thus

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right) = \left(\frac{b}{p_1}\right) \left(\frac{b}{p_2}\right) \cdots \left(\frac{b}{p_k}\right) = \left(\frac{b}{P}\right)$$

by Proposition 6.1.1. This proves (1). In a very similar way (2) follows from Proposition 6.1.2, and (3) straight from the definition of Jacobi symbol. ▽

6.8 The Generalized Law of Quadratic Reciprocity Suppose $P, Q > 0$ are odd.

1. $\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2}}$
2. $\left(\frac{2}{P}\right) = (-1)^{\frac{P^2-1}{8}}$
3. $\left(\frac{P}{Q}\right) \left(\frac{Q}{P}\right) = (-1)^{\left(\frac{P-1}{2}\right)\left(\frac{Q-1}{2}\right)}$

No Proof. The proof is set aside as an independent assignment. ▽

Exercise. Evaluate $\left(\frac{a}{p}\right)$ with the help of Jacobi symbol.

1. $a = 21, p = 61$
2. $a = 35, p = 103$
3. $a = -69, p = 127$
4. $a = 816, p = 239$

6.9 Modular Square Root If a is a quadratic residue modulo $p \equiv 3 \pmod{4}$ then the congruence $x^2 \equiv a \pmod{p}$ has exactly two solutions given by $x \equiv \pm a^{(p+1)/4} \pmod{p}$.

Proof. Using Euler’s Criterion, $(a^{(p+1)/4})^2 = a^{(p+1)/2} = a^{(p-1)/2} a \equiv \left(\frac{a}{p}\right) a = a \pmod{p}$. Hence $x^2 \equiv a \pmod{p}$ implies $x \equiv \pm a^{(p+1)/4} \pmod{p}$ by Problem 3.14 and these two solutions are distinct since $p \nmid 2a$. ▽

Exercise. Find all solutions.

1. $x^2 \equiv 2 \pmod{23}$
2. $x^2 - 2x + 3 \equiv 0 \pmod{11}$
3. $x^2 \equiv 10 \pmod{21}$
4. $x^2 \equiv 31 \pmod{55}$

Problem Set 6

1. Find all the quadratic residues and non-residues modulo 11.
2. Evaluate the Legendre symbol $\left(\frac{7}{11}\right)$ using (a) Euler's Criterion (b) Gauss' Lemma (c) Eisenstein's Lemma (d) Quadratic Reciprocity Law.
3. Does the congruence $x^2 \equiv 186 \pmod{557}$ have a solution?
4. Does the congruence $x^2 - 6x \equiv 2 \pmod{79}$ have a solution?
5. Does the congruence $x^2 - 5x + 2 \equiv 0 \pmod{29}$ have a solution?
6. Evaluate the Jacobi symbol $\left(\frac{218}{385}\right)$.
7. Characterize the prime numbers modulo which 5 is a quadratic residue.
8. Find all solutions of the congruence $x^2 \equiv 8 \pmod{31}$.
9. Find all solutions of the congruence $2x^2 + x + 2 \equiv 0 \pmod{31}$.
10. Find all solutions of the congruence $x^2 \equiv 29 \pmod{35}$.
11. Investigate true or false.
 - (a) $\left(\frac{713}{1009}\right) = 1$ thus 713 is a quadratic residue modulo 1009.
 - (b) $\left(\frac{442}{751}\right) = -1$ thus 442 is a quadratic non-residue modulo 751.
 - (c) $\left(\frac{2}{15}\right) = 1$ thus 2 is a quadratic residue modulo 15.
 - (d) $\left(\frac{7}{15}\right) = -1$ thus 7 is a quadratic non-residue modulo 15.
12. Suppose that a is relatively prime to an odd prime p . Prove that the congruence $x^2 \equiv a \pmod{p}$ has either exactly two solutions or none.
13. Prove that -1 is a quadratic residue modulo $p > 2$ if and only if $p \equiv 1 \pmod{4}$.
14. Prove that 2 is a quadratic residue modulo $p > 2$ if and only if $p \equiv \pm 1 \pmod{8}$.
15. Prove that -2 is a quadratic residue modulo $p > 2$ if and only if $p \equiv 1, 3 \pmod{8}$.
16. Prove that -3 is a quadratic residue modulo $p > 2$ if and only if $p \equiv 1 \pmod{6}$.

Project 6 Electronic Coin Tossing

In a game of coin tossing, two players have a fifty-fifty chance of winning by betting on the outcome, either Head or Tail. How can this game be played electronically, over email for instance?

Alia knows two large primes $p \equiv q \equiv 3 \pmod{4}$ and sends the product $n = pq$ to Bob. In turn Bob chooses an integer $h < n$ and sends $a = h^2 \% n$ to Alia. Using 6.9 and Chinese Remainder Theorem, Alia is able to solve $x^2 \equiv a \pmod{n}$ and finds four roots in the forms $x \equiv \pm h, \pm t \pmod{n}$. Alia now guesses Bob's number, either h or t . If Alia sends h to Bob, Alia wins. If, however, she picks t then Bob wins and he proves it by returning to her the factors p, q , one of which equals $\gcd(h + t, n)$, hence can be computed in no time using the Euclidean Algorithm.

Exercise. Verify that the congruence $x^2 \equiv a \pmod{pq}$ has indeed four roots whose residues mod pq equal $h, pq - h, t, pq - t$. Also prove that $\gcd(h + t, pq) = p$ or q .

Assignment. Illustrate the above discussion using h your 6-digit PUN and $n = 999697$, which supposedly you have factored into two primes back in Project 4. First compute $a = h^2 \% n$ then find the four roots of $x^2 \equiv a \pmod{n}$ and finally verify that $\gcd(h + t, n)$ is one of the two prime factors of n .

To Learn More

Any one of the following textbooks is recommended for further reading and self-study.

1. David M. Burton, *Elementary Number Theory*, Sixth Edition 2007, McGraw Hill.
2. Joseph H. Silverman, *A Friendly Introduction to Number Theory*, Third Edition 2006, Prentice Hall.
3. Kenneth H. Rosen, *Elementary Number Theory and Its Applications*, Fifth Edition 2005, Addison Wesley.
4. Niven, Zuckerman, and Montgomery, *An Introduction to the Theory of Numbers*, Fifth Edition 1991, Wiley.

Answers & Hints

<p>Problem Set 1</p> <ol style="list-style-type: none"> 1. No, 2 2. $111 \% 24 = 15$ 3. 1, 5, 7, 11 4. 3 5. $(-21, 13)$ 6. $(3 - 13k, 3 + 5k)$ 7. 7 and 3 minutes 8. F F T F T 9. T T F T F 10. Use 1.5.2 11. Start: n is even or odd 12. Start: n is even or odd 13. Start: $n = 2k + 1$ 14. Use 1.2 and 1.6.4 15. Use Problems 13 and 14 16. $(n-2)(n-1)n(n+1)(n+2)$ then use 1.2 and 1.6.4 	<p>Problem Set 2</p> <ol style="list-style-type: none"> 7×35759 18 total 120 8 pairs total 2, 5, 17, 37 $3 + 2003, 7 + 1999, \dots$ 3, 7, 31, 127, 8191 3, 5, 17, 257, 65537 $\approx 7.8 \times 10^4$ $\approx 4.0 \times 10^8$ F F T T T $\text{lcm}(m, n) \cdot \text{gcd}(m, n) = mn$ Use 2.3 Use 2.4 3, 5, 7 Like 2.6 with $6(N - 1) + 5$ 	<p>Problem Set 3</p> <ol style="list-style-type: none"> 1, 3, 5, 7, 9, 11, 13, 15, 17 2, 3, 5, 11, 19 $x \equiv 6 \pmod{9}$ 7 1, 5, 7, 11 1002 $x \equiv 1537 \pmod{3960}$ 2.62 dinars T T T T F Use 3.7 Use 3.7 and find inverse Start: $a \equiv 1, 3, 5, 7 \pmod{8}$ Start: $p = 3k + 1$ Like 3.6 See Problem 2.12 Show $(n - 1)! \equiv 0 \pmod{n}$
<p>Problem Set 4</p> <ol style="list-style-type: none"> 1. 1, 5, 7, 11, 13, 17, 19, 23 2. 1, 7, 11, 13, 17, 19, 23, 29 3. 214548 4. 5, 8, 10, 12 5. 70 6. 34 7. 6 8. 69 9. 75 10. F T T F 11. Use 3.14 12. Use 3.3 13. Check! 14. Use 4.6 and 4.7 15. Use 4.7.3 16. Use Problem 15 	<p>Problem Set 5</p> <ol style="list-style-type: none"> 10 No 3 and 7 3, 2, 3, 6, 1 $2^3, 2^7, 2^9$ No 200 7, 17, 31 $x \equiv 4 \pmod{12}$ F F F T Use 4.7 and 5.1.2 Prove $(a^{-1})^k = (a^k)^{-1}$ Use 3.6 and 4.3 $4 = 2^2$ and use Problem 13 Use Problem 13 Use Problem 13 	<p>Problem Set 6</p> <ol style="list-style-type: none"> 1, 3, 4, 5, 9 & 2, 6, 7, 8, 10 -1 No Yes No -1 $p \equiv \pm 1 \pmod{5}$ 15 and 16 22 and 24 8, 13, 22, 27 T T F T Use Problem 3.14 Use 6.2 Use 6.5 Use Problems 13 and 14 Use 6.2 and 6.6

Primes < 4,000

2	3	5	7	11	13	17	19	23	29	31
37	41	43	47	53	59	61	67	71	73	79
83	89	97	101	103	107	109	113	127	131	137
139	149	151	157	163	167	173	179	181	191	193
197	199	211	223	227	229	233	239	241	251	257
263	269	271	277	281	283	293	307	311	313	317
331	337	347	349	353	359	367	373	379	383	389
397	401	409	419	421	431	433	439	443	449	457
461	463	467	479	487	491	499	503	509	521	523
541	547	557	563	569	571	577	587	593	599	601
607	613	617	619	631	641	643	647	653	659	661
673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823
827	829	839	853	857	859	863	877	881	883	887
907	911	919	929	937	941	947	953	967	971	977
983	991	997	1009	1013	1019	1021	1031	1033	1039	1049
1051	1061	1063	1069	1087	1091	1093	1097	1103	1109	1117
1123	1129	1151	1153	1163	1171	1181	1187	1193	1201	1213
1217	1223	1229	1231	1237	1249	1259	1277	1279	1283	1289
1291	1297	1301	1303	1307	1319	1321	1327	1361	1367	1373
1381	1399	1409	1423	1427	1429	1433	1439	1447	1451	1453
1459	1471	1481	1483	1487	1489	1493	1499	1511	1523	1531
1543	1549	1553	1559	1567	1571	1579	1583	1597	1601	1607
1609	1613	1619	1621	1627	1637	1657	1663	1667	1669	1693
1697	1699	1709	1721	1723	1733	1741	1747	1753	1759	1777
1783	1787	1789	1801	1811	1823	1831	1847	1861	1867	1871
1873	1877	1879	1889	1901	1907	1913	1931	1933	1949	1951
1973	1979	1987	1993	1997	1999	2003	2011	2017	2027	2029
2039	2053	2063	2069	2081	2083	2087	2089	2099	2111	2113
2129	2131	2137	2141	2143	2153	2161	2179	2203	2207	2213
2221	2237	2239	2243	2251	2267	2269	2273	2281	2287	2293
2297	2309	2311	2333	2339	2341	2347	2351	2357	2371	2377
2381	2383	2389	2393	2399	2411	2417	2423	2437	2441	2447
2459	2467	2473	2477	2503	2521	2531	2539	2543	2549	2551
2557	2579	2591	2593	2609	2617	2621	2633	2647	2657	2659
2663	2671	2677	2683	2687	2689	2693	2699	2707	2711	2713
2719	2729	2731	2741	2749	2753	2767	2777	2789	2791	2797
2801	2803	2819	2833	2837	2843	2851	2857	2861	2879	2887
2897	2903	2909	2917	2927	2939	2953	2957	2963	2969	2971
2999	3001	3011	3019	3023	3037	3041	3049	3061	3067	3079
3083	3089	3109	3119	3121	3137	3163	3167	3169	3181	3187
3191	3203	3209	3217	3221	3229	3251	3253	3257	3259	3271
3299	3301	3307	3313	3319	3323	3329	3331	3343	3347	3359
3361	3371	3373	3389	3391	3407	3413	3433	3449	3457	3461
3463	3467	3469	3491	3499	3511	3517	3527	3529	3533	3539
3541	3547	3557	3559	3571	3581	3583	3593	3607	3613	3617
3623	3631	3637	3643	3659	3671	3673	3677	3691	3697	3701
3709	3719	3727	3733	3739	3761	3767	3769	3779	3793	3797
3803	3821	3823	3833	3847	3851	3853	3863	3877	3881	3889
3907	3911	3917	3919	3923	3929	3931	3943	3947	3967	3989